An Environment for Developing Secure Software

Secure

I nternet

Programming

Languages

New Ideas

- Static security analysis for software
- Tools for inferring security properties of code
- Provably secure programming languages
- Treat secure flow analysis as type checking
- Application of type inference to security

Impact

- Secure programing languages for thin-client/server applications, e.g. Army Java boxes and Java-based command and control such as Navy JMCIS-Ashore
- Will allow software to be analyzed and "certified" to meet specific security properties
- Safe and secure features of programming languages for extensible architectures and active networks

Schedule

Milestones	FY97	FY98
Development of secure information flow type system without/with non-termination & exceptions	w/o NT&E	with NT&E
Establish soundness of type system		
Investigate notion of principal security typing		
Develop type system inference algorithm		
Develop tool implementing algorithm		
Final Report		

U.S. Naval Postgraduate School Center for INFOSEC Studies and Research